CLAIMS

What is claimed is:

1. A dual-tapped buffer ladder comprising any number of cascading of the following:

a pair of D-type flip flops having D and L inputs;

a plurality of cascaded upper buffers having a predetermined delay d_1 and respective output taps;

a plurality of cascaded lower buffers having a predetermined delay d_2, and respective output taps, wherein $d_1 \neq d_2$;

a first one of the pair of D-type flip flops having its D and L inputs connected to a respective output tap of the upper buffer and a respective output tap of the lower buffer;

a second one of the pair of D-type flip flops 215 having its D and L inputs connected to a respective output tap of one of the lower buffers and a respective output of one of the upper buffers;

a common clock input connected to an input of the first buffers of both the plurality of cascaded upper buffers and the plurality of cascaded lower buffers;

wherein a delay difference between the cascaded upper buffers $n*d_1$ and cascaded lower buffers $n*d_2$ changes along different positions of the ladder circuit.

2. The dual-tapped buffer ladder according to claim 1, further comprising:

more than one pair of D-type flip flops being arranged in a ladder arrangement; and

a number of respective cascaded upper buffers and cascaded lower buffers corresponds to a number of D-type flip flops.

3. A random number generator comprising a sequence of cascading:

pairs of D-type flip-flops having D and L inputs;

cascaded upper buffers having a predetermined delay d_1 and respective output taps;

cascaded lower buffers having a predetermined delay d_2, and respective output taps, wherein $d_1 \neq d_2$;

a first one of the pair of D-type flip flops 205 having its D and L inputs connected to a respective output tap of one of the cascaded upper buffers and a respective output tap of one of the cascaded lower buffers;

a second one of the pair of D-type flip flops having its D and L inputs connected to a respective output tap of one of the lower buffers and a respective output of one of the upper buffers

a common clock input connected to an input of the first one of both the cascaded upper buffers and the cascaded lower buffers;

a metastability detector for each individual flip-flop, a respective metastability detector connected to the Q output of each respective flip-flop;

said metastability detectors having a counting feature to count a number of times that each of the respective metastability detector signals a metastable state;

wherein one flip-flop of the pair flip-flops is selected to generate a random numbers from its output.

4. The random number generator according to claim 3, wherein the flip-flop having the highest metastable count is selected as the source of the random number generator.

5. The random number generator according to claim 4, wherein periodically the counters of the metastability detector are reset so that a flip-flop having the most recent highest number of metastable events is selected for random number generation.

6. The random number generator according to claim 3, wherein a delay difference between the cascaded upper buffers of individual delay d_1 and cascaded lower buffers of individual delay d_2 changes along different positions of the ladder circuit.

7. The random number generator according to claim 4, wherein the counters of the metastability detector are reset each time the frequency of the metastable events of the selected flip-flop changes.

8. A smart card having the random number generator according to claim 4.

9. The random number generator according to claim 4, wherein the delays d_1 and d_2 determine the number of pairs of flip-flopsin the ladder arrangement to assure continuous functioning regardless of environmental changes.

10. The random number generator according to claim 3, wherein data change respective to a clock at time points selected to violate setup and hold times of particular flip-flops being used.

11. A method for providing a dual-tapped buffer ladder comprising:

(a) providing a pair of D-type flip flops having D and L inputs;

(b) connecting a sequence of substantially identical cascaded upper buffers having a predetermined delay d_1 and respective output taps to one of the D and L inputs of the pair of D-type flip-flops;

(c) connecting a sequence of substantially identical cascaded lower buffers having a predetermined delay d_2, and respective output taps to the other of the D and L inputs connected in step (b), wherein $d_1 \neq d_2$;

(d) connecting a common clock input to the first inputs of both the cascaded upper buffers and the cascaded lower buffers;

wherein a delay difference between the cascaded upper buffers of individual delay d_1 and cascaded lower buffers of individual delay d_2 changes along different positions of the ladder circuit.

12. The method of claim 11, further comprising:

connecting more than one pair of D-type flip flops in a ladder arrangement; and

connecting a number of respective cascaded upper buffers and cascaded lower buffers to correspond to a number of D-type flip flops.

13. A method for random number generation comprising:

(a) providing a pair of D-type flip flops having D and L inputs;

(b) connecting substantially identical cascaded upper buffers each having a predetermined delay d_1 and respective output taps to one of the D and L inputs of the pair of D-type flip-flops;

(c) connecting substantially identical cascaded lower buffers each having a predetermined delay d_2, and respective output taps to the other one of the D and L inputs of the pair of D-type flip-flops, wherein $d_1 \neq d_2$;

(d) connecting a common clock to the first inputs of both of the cascaded upper buffers and the cascaded lower buffers;

(e) providing a metastability detector for each individual flip-flop of the pair of flip flops, a respective metastability detector connected to the Q output of each respective flip-flop;

(f) said metastability detectors counting a number of times that each of the respective metastability detector signals a metastable state; and

(g) selecting one flip-flop of the pair flip-flops is selected to generate a random numbers from its output.

14. The method according to claim 13, wherein the flip-flop selected in step (g) to provide an input to a random number generator has the highest metastable count.

15. The method according to claim 14, further comprising (h) periodically resetting the counters of the metastability detector according to predetermined criteria and returning to step (g).

16. The method according to claim 15, wherein the predetermined criteria used to reset the counters comprises changing of the frequency of the metastable events of the selected flip-flop.

17. The method according to claim 13, wherein a delay difference between the cascaded upper buffers and cascaded lower buffers is variable by changing the position where flip-flops are connected to a ladder arrangement of buffers.

18. The method according to claim 14, wherein the difference of delays d_1 and d_2 corresponds to the number of pairs of flip-flops in the ladder arrangement.

19. The method according to claim 13, wherein data signals connected in step (c) have delay values selected to violate setup and hold times of particular flip-flops being used.